CLAIMS

1. A decoder for processing a transport packet stream comprising packetised data encapsulated within the packet payloads, said decoder comprising:

means for receiving an identifier of a particular security module system from a portable security module;

means for configuring the decoder in response to the received identifier;

means for receiving filter data for filtering packetised data associated with said particular security module system from the portable security module; and

means for filtering said packetised data in response to said received filter data.

2. A decoder according to Claim 1, wherein the filtering means is configurable by said configuring means to extract from the packetised data data associated with said particular security module system for subsequent filtering in response to said received filter data.

3. A decoder according to Claim 1, wherein said identifier comprises an identifier of a particular conditional access system.

4. A decoder according to Claim 3, wherein the filtering means is adapted to extract from the packetised data transport packets containing a program map table and a conditional access table.

5. A decoder according to Claim 4, wherein the configuring means is adapted to receive the program map table and conditional access table from the filtering means and configure the filtering means in response to the received identifier and data contained in the program map table and the conditional access table.

6. A decoder according to Claim 1, wherein said identifier comprises an identifier of a particular debiting system used by the security module.

7. A decoder according to Claim 1, wherein said identifier comprises an identifier of a particular crediting system used by the security module.

8. A decoder according to Claim 1, wherein the filtering means is configurable in response to filter data comprising at least a table identifier or a section identifier for the packetised data.

9. A decoder according to Claim 1, wherein the filtering means comprises first filtering means for extracting from the packetised data data associated with said particular security module system and second filtering means for filtering the extracted data in response to said filter data.

10. A decoder for processing a transport packet stream comprising packetised data encapsulated within the packet payloads, said decoder comprising:

first filtering means for extracting from the packetised data data associated with a particular security module system; and

second filtering means for filtering the extracted data in response to filter data received from a portable security module.

11. A decoder according to Claim 10, wherein the first filtering means is configurable in response to an identifier of said particular security module system received from said security module.

12. A decoder according to Claim 9, wherein said second filtering means comprises a plurality of filters, at least one of said filters being configurable in response to said filter data.

13. A decoder according to Claim 9, wherein said second filtering means is configurable in response to a data pattern included in said filter data.

14. A decoder according to Claim 13, wherein said second filtering means is configurable to filter from the extracted data data having a pattern matching said data pattern included in the filter data.

15. A decoder according to Claim 13, wherein said second filtering means is configurable to not filter from the extracted data data having a pattern matching said data pattern included in the filter data.

16. A decoder according to Claim 13, wherein said second filtering means is configurable to ignore at least part of said data pattern in response to a data masking pattern included in said filter data.

17. A decoder according to Claim 1, comprising means for forwarding to the security module conditional access data included in the packetised data.

18. A decoder according to Claim 17, wherein the conditional access data forwarded to the security module comprises entitlement control messages (ECMs) and/or entitlement management messages (EMMs).

19. A decoder according to Claim 1, wherein the filter data provided by the security module comprises data used by the filtering means to extract group and/or individual entitlement management messages addressed to the security module.

20. A decoder according to Claim 17, wherein the decoder is adapted to receive a control word generated by the security module in response to the conditional access data forwarded thereto, the control word being used by the decoder to descramble a scrambled transmission.

21. A decoder according to any Claim 1 adapted to encrypt and/or decrypt communications to and from the portable security module.

22. A portable security module for use with a decoder as claimed in Claim 1, said security module comprising memory means for storing an identifier of a particular system of the security module and means for communicating the identifier to the decoder to configure the decoder.

23. A portable security module according to Claim 22, comprising means for storing filter data and means for communicating the filter data to filtering means in the decoder.

24. A portable security module according to Claim 22 comprising a smartcard.

25. A method of processing a transport packet stream comprising packetised data encapsulated within the packet payloads, said method comprising the steps at a decoder of:

receiving an identifier of a particular security module system from a portable security module;

configuring the decoder in response to the received identifier;

receiving filter data for filtering packetised data associated with said particular security module system from the portable security module; and

filtering said packetised data in response to said received filter data.

26. A method according to Claim 25, wherein the packetised data is filtered to extract data associated with said particular security module system.

27. A method according to Claim 25, wherein said identifier comprises an identifier of a particular conditional access system.

28. A method according to Claim 27, wherein transport packets containing a program map table and a conditional access table are extracted from said packetised data.

29. A method according to Claim 28, wherein the packetised data is filtered in response to the received identifier and data contained in the program map table and the conditional access table.

30. A method according to Claim 25, wherein said identifier comprises an identifier of a particular debiting system used by the security module.

31. A method according to Claim 25, wherein said identifier comprises an identifier of a particular crediting system used by the security module

32. A method according to Claim 25, wherein the filter data comprises at least a table identifier or a section identifier for the packetised data.

33. A method according to Claim 25, wherein the packetised data is filtered according to a data pattern included in the filter data.

34. A method according to Claim 33, wherein data having a pattern matching said data pattern is filtered from the packetised data.

35. A method of processing a transport packet stream comprising packetised data encapsulated within the packet payloads, said method comprising the steps at a decoder of:

extracting from the packetised data data associated with a particular security module system; and

filtering the extracted data in response to filter data received from a portable security module.

36. A method according to Claim 35, wherein an identifier of said particular security module system is received from said security module.

37. A method according to Claim 25, wherein conditional access data included in the extracted data is forwarded to the security module.

38. A method according to Claim 37, wherein the conditional access data forwarded to the security module comprises entitlement control messages (ECMs) and/or entitlement management messages (EMMs).

39. A method according to Claim 25, wherein the filter data provided by the security module comprises data used by the decoder to extract group and/or individual entitlement management messages addressed to the security module.

40. A method according to Claim 37, wherein the a control word is generated by the security module in response to the conditional access data forwarded thereto, the control word being used by the decoder to descramble a scrambled transmission.